IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellants:	Raymond E. SUORSA et al.	§	Confirmation No.:	9527
		§		
Serial No.:	09/838,135	§	Group Art Unit:	2145
		§		
Filed:	April 20, 2001	§	Examiner:	T. M. Hossain
		§		
For:	Automated Provisioning	§	Docket No.:	200704494-1
	Of Computer Networks	§		
	Using A Network	§		
	Database Data Model	§		

APPEAL BRIEF

Mail Stop Appeal Brief – Patents   Date: March 21, 2011
Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

Appellants hereby submit this Appeal Brief in connection with the above-identified application. A Notice of Appeal was electronically filed on January 20, 2011.

TABLE OF CONTENTS

I.   REAL PARTY IN INTEREST

The real party in interest is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 11445 Compaq Center Drive West, Houston, Texas, 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

II.   RELATED APPEALS AND INTERFERENCES

A Notice of Appeal was previously filed on December 28, 2009, and a corresponding Appeal Brief was filed on February 27, 2010 that resulted in reopening of prosecution.

III.   **STATUS OF THE CLAIMS**

Originally filed claims: 1-64.

Claim cancellations: 3.

Added claims: 65.

Presently pending claims: 1-2 and 4-65.

Presently appealed claims: 1-2 and 4-65.

IV.   STATUS OF THE AMENDMENTS

No amendments were filed after the Final Office Action of December 2, 2010.

V.   SUMMARY OF THE CLAIMED SUBJECT MATTER

This section provides a concise explanation of the subject matter defined in each of the independent claims, referring to the specification by page and line number or to the drawings by reference characters as required by 37 C.F.R. § 41.37(c)(1)(v).   Each element of the claims is identified with a corresponding reference to the specification or drawings where applicable.   The specification references are made to the application as filed by Appellants.   Note that the citation to passages in the specification or drawings for each claim element does not imply that the limitations from the specification and drawings should be read into the corresponding claim element.   Also note that these specific references are not exclusive; there may be additional support for the subject matter elsewhere in the specification and drawings.

Dissemination of information over the Internet typically involves use of web sites.[1]   Each web site requires an infrastructure (*e.g.*, site content storage, web servers, application servers, etc.) at one of more centralized locations connected to the Internet.[2]   Each server supporting a web site is provisioned with software necessary for the site.[3]   Provisioning includes installation and configuration of operating system and application software necessary for the site, and loading of site content.[4]

In the past, provisioning was often carried out manually.[5]   However, manual provisioning is time-consuming and prone to error.[6]   To overcome the shortcomings of manual provisioning, various techniques of automatic software

---

[1] P. 1, ¶ [0003], lines 1-9.

[2] P. 1-2, ¶ [0003], lines 9-21.

[3] P. 2, ¶ [0005], lines 3-6.

[4] P. 2, ¶ [0005], lines 6-9; p. 3, ¶ [0006], lines 1-11.

[5] P. 3, ¶ [0007], lines 1-2.

[6] P. 3-4, ¶ [0007], lines 3-15.

deployment have been developed.[7] For example, in an enterprise where all of the users interact with the same legacy applications, a "cookie cutter" type of approach, where every computer has the same set of programs, can be used to deploy the software.[8] Once the programs and settings have been determined, they can be packaged in a fixed format (*i.e.*, a "ghost" or "brick"), and automatically disseminated to all of the appropriate computers.[9]

The cookie cutter approach is not effective in situations where computers need to be customized to accommodate individual requirements of varied users.[10] In a data center housing many different web sites, each site likely uses different business logic requiring different combinations of hardware and software.[11] Appellants have devised agent-based techniques for provisioning computers that overcome the aforementioned deficiencies of the prior art.[12]

The invention of claim 1 is directed to a method for automated provisioning of computer networks. The method includes receiving, by a network device to be provisioned, at least one unsolicited software retrieval command to be executed on the network device.[13] The command is sent by a secure provisioning network 31 connected via a network to the network device.[14] The provisioning network reads parameters of the network device from a network database 32.[15] The reading is responsive to an inquiry based on the at least one command and

---

[7] P. 4, ¶ [0009], lines 1-4.

[8] P. 4, ¶ [0009], lines 5-8.

[9] P. 4, ¶ [0009], lines 9-11.

[10] P. 5, ¶ [0010], lines 1-3.

[11] P. 5, ¶ [0010], lines 5-17.

[12] P. 6, ¶¶[0012], lines 1-9.

[13] Fig. 7, p. 17, ¶ [0049], lines 1-3.

[14] Figs. 6-7; p. 16, ¶ [0047], lines 4-6; p. 18-19, ¶ [0051], lines 14-15.

[15] Fig. 7; p. 16, ¶ [0047], lines 11-19; p. 18, ¶ [0051], lines 7-9.

received from the network device.[16]   The provisioning network determines whether the at least one command can be properly executed on the network device based upon the parameters read.[17]   The network device executes the at least one command only if it is determined that the at least one command can be properly executed.[18]

---

[16] P. 18, ¶ [0051], lines 4-9.

[17] P. 18, ¶ [0051], lines 7-9.

[18] P. 19, ¶ [0051], lines 20-24.

VI.   GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 1, 2 and 4-65 are anticipated under 35 U.S.C. § 102(e) by Moshir (U.S. Pub. No. 2002/0100036, hereinafter "*Moshir*").

VII.   ARGUMENT

A.   Rejections Under 35 U.S.C. § 102(e) Over *Moshir*

1.   Claim 1

Independent claim 1 requires "receiving, by a network device to be provisioned, at least one unsolicited software retrieval command, sent by a secure provisioning network connected via a network to the network device, to be executed on said network device." The Examiner cited *Moshir* Abstract, and ¶¶ [0062]-[0064] as allegedly teaching these limitations.

The *Moshir* Abstract teaches "updating . . . computers across a network without storing the updates on an intermediate machine within the network. . . . The software update can be stored originally at an address that is inaccessible through the network firewall by intermediately uploading the software update to an update computer which is not a part of the network but has access through the firewall, which is then used to distribute the update."

Moshir ¶¶ [0062]-[0064] teach that after a download is stored in an update computer a second download 312 is attempted to download the software from the update server to the target computer. A monitor 302 checks the installation. If the installation fails 316, then the task that failed is suspended 318.

None of the portions of *Moshir* cited by the Examiner teach that the target computer (*i.e.*, the device to be provisioned) receives an unsolicited software retrieval command to be executed by the target. *Moshir* ¶ [0062] teaches that a second download 312 is attempted to download software to the target computer. However, *Moshir* fails to teach that the download 312 includes a "software retrieval command to be executed by the target computer, or that such a command is unsolicited.

Claim 1 also requires "reading, by said provisioning network, parameters of said network device from a network database, said reading being responsive to an inquiry based on the at least one unsolicited software retrieval command and received from said network device." The Examiner cited *Moshir* ¶¶ [0022]-[0024], [0031], [0059], and [0086]-[0087] as allegedly teaching these limitations. *Moshir* ¶¶ [0022]-[0024] teach an inventory library database 918 that contains hardware

and software information about each target computer. The update server 528 uses the information to present the user with patch status reports for all computers in the network.

Moshir ¶ [0031] teaches an update agent 204 that surveys its own target computer. The information provided by the update agent 204 is stored in a database at another location and used to determine what updates a target computer needs.

Moshir ¶ [0059] teaches that a task id is placed on an update task list 222 if a condition is met (*e.g.*, patch not on target computer, permission, etc). The task specifies a software update download address.

Moshir ¶¶ [0086]-[0087] teach that the inventory library 918 contains target computer hardware and software information provided by a discovery agent 548 on the target computer.

Thus, while *Moshir* teaches a library of target computer information useable to determine what updates a target computer needs[19] and to generate reports,[20] *Moshir* fails to teach reading the information "responsive to an inquiry . . . received from the" target computer, or that such an "inquiry [is] is based on the at least one unsolicited software retrieval command" received by the device being provisioned (*i.e.*, the target computer).

Claim 1 further requires "determining, by said provisioning network, whether the at least one unsolicited software retrieval command can be properly executed on said network device based upon the parameters read." The Examiner cited *Moshir* ¶¶ [0078]-[0083] and [0088] as allegedly teaching these limitations.

Moshir ¶¶ [0078]-[0083] teach that a patch fingerprint includes inventory install dependencies 912 describing hardware and software required on a target computer for installation of the patch. A signature block 910 of the patch fingerprint is sent to the target computer to request return of specific install

---

[19] *Moshir*, ¶ [0022].

[20] *Moshir*, ¶ [0024].

information. The evaluator 914 uses the returned specific install information to determine if the patch is absent on the target computer. Thus, while *Moshir* teaches determining whether a patch can be installed on a target computer, *Moshir* fails to teach that the determination is "based on the parameters read" responsive to an inquiry received from the target computer as claim 1 requires.

Moshir ¶ [0088] teaches a report generator 922 that provides a user with network computer patch status reports. The reports identify computers needing a patch, computers already patched, and computers that can't receive the patch until upgraded. *Moshir* fails to teach that report generation is "based on the parameters read" responsive to an inquiry received from the target computer as claim 1 requires.

Moreover, Appellants respectfully submit that *Moshir* is not a proper reference under 35 U.S.C. § 102(e) with regard to the presently considered claim limitations. *Moshir* was filed September 20, 2001 and claims priority to provisional application No. 60/234,680 filed on September 22, 2000 (hereinafter "*Moshir Prov.*"). Appellants assume that the Examiner is relying on the provisional filing date to establish *Moshir* as a § 102(e) reference because the present application pre-dates the *Moshir* filing date. The Court of Appeals for the Federal Circuit has determined that an important limitation to the application of a provisional filing date to prospective § 102(e) art is "that the provisional application must provide written description support for the claimed invention."[21] The Examiner has failed to identify written description support for the present limitations in the provisional application, and Appellants have been unable to identify any such support. More specifically, the *Moshir Prov.* provides no support patch fingerprints, signature blocks, or using these or any other resources to determine whether a software retrieval command can be properly executed based on parameters read from a network database.

---

[21] *In re Giacomini*, No. 2009-1400, 2010 WL 2674461, at *3 (CAFC July 7, 2010).

Claim 1 yet further requires "executing the at least one unsolicited software retrieval command on said network device only if it is determined that the at least one unsolicited software retrieval command can be properly executed." The Examiner cited *Moshir* ¶¶ [0088]-[0101] as allegedly teaching these limitations. *Moshir* ¶ [0088] is explained above.

Moshir ¶¶ [0089]-[0101] describe the discovery agent, and discloses deciding if a software program can be installed by verifying that the necessary hardware/software is present.

Appellants respectfully submit that *Moshir* is not a proper reference under 35 U.S.C. § 102(e) with regard to the presently considered claim limitations. The Examiner has failed to identify written description support for the present limitations in the provisional application, and Appellants have been unable to identify any such support. More specifically, the *Moshir Prov.* provides no support for a "discovery agent" or for "executing the at least one unsolicited software retrieval command on said network device only if it is determined that the at least one unsolicited software retrieval command can be properly executed."

For at least these reasons, *Moshir* fails to teach the limitations of independent claim 1. Therefore, Appellants respectfully submit the that Examiner erred in rejecting all pending claims and request that the rejections of the claims 1, 2 and 4-65 be reversed, and the claims set for issue.

2. Claim 2

Claim 2 requires "the at least one unsolicited software retrieval command is executed by an agent on said network device, the agent being configured to manipulate all of the software on the network device." The Examiner cited *Moshir* ¶ [0020] as allegedly teaching these limitations. The cited portion of *Moshir* teaches that "an update agent running on [a computer] may connect to an update server, and then process whatever tasks the administrator has designated for that agent." Thus, *Moshir* teaches an agent that can perform designated tasks. However, *Moshir* fails to expressly or inherently teach that the designated tasks encompass manipulation of all of the software on the computer as required by

claim 2. For at least these additional reasons, Appellants respectfully submit that the Examiner erred in rejecting claim 2.

3. Claim 4

Claim 4 requires "verifying the validity of the at least one unsolicited software retrieval command by requesting verification from the secure provisioning network." The Examiner cited *Moshir* ¶ [0088] as allegedly teaching these limitations. The cited portion of *Moshir* teaches report generation, and fails to teach "verifying the validity of [a] . . . software retrieval command" or "requesting verification from the secure provisioning network." For at least these additional reasons, Appellants respectfully submit that the Examiner erred in rejecting claim 4 and all claims depending therefrom.

4. Claim 6

Claim 6 requires "the step of determining [of claim 1] is based on reading software packaging parameters." The Examiner cited *Moshir* ¶ [0081] as allegedly teaching these limitations. The cited portion of *Moshir* teaches a discovery agent 548 on a target computer gathering target computer information and sending the information to a repository component 818. Appellants respectfully submit that target computer information is not "software packaging parameters." For at least this additional reason, Appellants respectfully submit that the Examiner erred in rejecting claim 6 and all claims depending therefrom.

5. Claim 8

Claim 8 requires "the software packaging parameters comprise software roles." The Examiner cited *Moshir* ¶¶ [0024] and [0081] as allegedly teaching these limitations. *Moshir* ¶ [0024] teaches that the inventory database collects an inventory of software installed on a target computer. *Moshir* ¶ [0081] is explained above. Neither cited portion of *Moshir* teaches software roles as required by the present claim and explained in the specification.[22] "[T]he PTO's "broadest" interpretation must be reasonable, and must be in conformity with the invention

---

[22] *E.g.*, Specification, ¶ [0057].

as described in the specification."[23] For at least this additional reason, Appellants respectfully submit that the Examiner erred in rejecting claim 8 and all claims depending therefrom.

6.   Claim 58

Claim 58 requires "the step of executing the at least one unsolicited software command is limited to entities having an approved access level to execute the at least one command." The Examiner cited *Moshir* ¶ [0070] as allegedly teaching these limitations. *Moshir* ¶ [0070] teaches guest, regular and executive user levels for accessing the help desk services at the PatchLink website. An executive member can use more advanced features of the site than regular or guest members. However, *Moshir* fails to teach that execution of a software retrieval command is limited to entities having an approved access level. Instead, *Moshir* ¶ [0070] teaches that help desk functions of a website are restricted based on user access levels. Restricting website functionality available to users based on user levels is different from limiting network device execution of a software retrieval command based to entities having an approved access level. For at least this additional reason, Appellants respectfully submit that the Examiner erred in rejecting claim 58 and all claims depending therefrom.

7.   Claim 65

Claim 65 requires "the step of determining [of claim 1] is based upon an identification of a virtual local area network (VLAN) with which said network device is associated." The Examiner cited *Moshir* ¶¶ [0046] and [0052] as allegedly teaching these limitations. *Moshir* ¶ [0046] teaches that term "internet" includes a "virtual private network," and may be configured according to the invention of *Moshir*. *Moshir* ¶ [0052] teaches firewalls. Neither cited portion of *Moshir* teaches basing determining of whether a software retrieval command can be properly executed on identifying a VLAN with which a device is associated.

---

[23] *In re Vaidyanathan*, No. 2009-1404, 2010 WL 2000682, at *11, (Fed. Cir. May, 19, 2010).

For at least this additional reason, Appellants respectfully submit that the Examiner erred in rejecting claim 65.

B. Conclusion

For the reasons stated above, Appellants respectfully submit that the Examiner erred in rejecting all pending claims. It is believed that no extensions of time or fees are required, beyond those that may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. § 1.136(a), and any fees required (including fees for net addition of claims) are hereby authorized to be charged to Hewlett-Packard Development Company's Deposit Account No. 08-2025.

Respectfully submitted,

/David M. Wilson/

David M. Wilson
PTO Reg. No. 56,790
CONLEY ROSE, P.C.
(713) 238-8000 (Phone)
(713) 238-8008 (Fax)
ATTORNEY FOR APPELLANTS

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
Legal Dept., M/S 35
3404 E. Harmony Road
Fort Collins, CO 80528

VIII.   CLAIMS APPENDIX

1.   A method for automated provisioning of computer networks, comprising the steps of:

> receiving, by a network device to be provisioned, at least one unsolicited
>> software retrieval command, sent by a secure provisioning network
>>
>> connected via a network to the network device, to be executed on
>>
>> said network device;
>
> reading, by said provisioning network, parameters of said network device
>> from a network database, said reading being responsive to an
>>
>> inquiry based on the at least one unsolicited software retrieval
>>
>> command and received from said network device;
>
> determining, by said provisioning network, whether the at least one
>> unsolicited software retrieval command can be properly executed
>>
>> on said network device based upon the parameters read; and
>
> executing the at least one unsolicited software retrieval command on said
>> network device only if it is determined that the at least one
>>
>> unsolicited software retrieval command can be properly executed.

2.   The method of claim 1, wherein the at least one unsolicited software retrieval command is executed by an agent on said network device, the agent being configured to manipulate all of the software on the network device.

4.   The method of claim 1, further comprising:

verifying the validity of the at least one unsolicited software retrieval command by requesting verification from the secure provisioning network.

5.   The method of claim 4, wherein the step of verifying is accomplished by way of communicating with a communication gateway of the secure provisioning network.

6.   The method of claim 1, wherein the step of determining is based on reading software packaging parameters.

7.   The method of claim 6, wherein the software packaging parameters comprise compatibility requirements.

8.   The method of claim 6, wherein the software packaging parameters comprise software roles.

9.   The method of claim 7, wherein the compatibility requirements comprise software roles compatibility requirements.

10.   The method of claim 6, wherein the software packaging parameters comprise operating system (OS) parameters.

11.   The method of claim 7, wherein the compatibility requirements comprise operating system (OS) compatibility requirements.

12.   The method of claim 6, wherein the software packaging parameters comprise parameters regarding specific customer account requirements.

13.   The method of claim 7, wherein the compatibility requirements comprise requirements regarding specific customer account compatibility.

14.   The method of claim 8, wherein the software roles comprise customer account software roles.

15.   The method of claim 9, wherein the software roles compatibility requirements comprise customer account software roles compatibility requirements.

16.   The method of claim 6, wherein the software packaging parameters comprise device parameters.

17.   The method of claim 16, wherein the device parameters comprise device interface parameters.

18.   The method of claim 17, wherein the device interface parameters comprise device internet protocol (IP) address parameters.

19.   The method of claim 17, wherein the interface parameters comprise interface type parameters.

20.   The method of claim 16, wherein the device parameters comprise interface components parameters.

21.   The method of claim 16, wherein the device parameters comprise memory components parameters.

22.   The method of claim 16, wherein the device parameters comprise storage components parameters.

23.   The method of claim 16, wherein the device parameters comprise central processing unit (CPU) parameters.

24.   The method of claim 7, wherein the compatibility requirements comprise device compatibility requirements.

25.   The method of claim 24, wherein the device compatibility requirements comprise interface compatibility requirements.

26.   The method of claim 25, wherein the interface compatibility requirements comprise IP compatibility requirements.

27.   The method of claim 25, wherein the interface compatibility requirements comprise interface type compatibility requirements.

28.   The method of claim 24, wherein the device compatibility requirements comprise interface components compatibility requirements.

29.   The method of claim 24, wherein the device compatibility requirements comprise memory components compatibility requirements.

30.   The method of claim 24, wherein the device compatibility requirements comprise storage components compatibility requirements.

31.   The method of claim 24, wherein the device compatibility requirements comprise central processing unit (CPU) components compatibility requirements.

32.   The method of claim 8, wherein software roles compatibility requirements comprise device roles compatibility requirements.

33.   The method of claim 9, wherein the software roles comprise device roles.

34.   The method of claim 6, wherein the software packaging parameters comprise application packaging parameters.

35.   The method of claim 7 wherein the compatibility requirements comprise application compatibility requirements.

36.   The method of claim 8, wherein the software roles comprise application software roles.

37.   The method of claim 36, wherein the application software roles define a group of services.

38.   The method of claim 9, wherein the software roles compatibility requirements comprise application roles compatibility requirements.

39.   The method of claim 38, wherein the application roles compatibility requirements define a group of services.

40.   The method of claim 6, wherein the software packaging parameters relate to a variety of network service tiers.

41.   The method of claim 7, wherein the compatibility requirements are defined according to a variety of network service tiers.

42.   The method of claim 6, wherein the software packaging parameters are defined by way of configuration parameters.

43.   The method of claim 42, wherein the configuration parameters comprise device configuration parameters.

44.   The method of claim 42, wherein the configuration parameters comprise interface configuration parameters.

45.   The method of claim 42, wherein the configuration parameters comprise virtual IP address parameters.

46.   The method of claim 42, wherein the configuration parameters comprise component type parameters.

47.   The method of claim 42, wherein the configuration parameters comprise role configuration parameters.

48.   The method of claim 47, wherein the role configuration parameters comprise device role configuration parameters.

49.   The method of claim 48, wherein the device role configuration parameters comprise device role history configuration parameters.

50.   The method of claim 7, wherein the compatibility requirements comprise configuration compatibility requirements.

51.   The method of claim 50, wherein the configuration compatibility requirements comprise device configuration compatibility requirements.

52.   The method of claim 50, wherein the configuration compatibility requirements comprise interface configuration compatibility, requirements.

53.   The method of claim 50, wherein the configuration compatibility requirements comprise virtual IP address compatibility requirements.

54.   The method of claim 50, wherein the configuration compatibility requirements comprise component type configuration compatibility requirements.

55.   The method of claim 50, wherein the configuration compatibility requirements comprise role configuration compatibility requirements.

56.   The method of claim 55, wherein the role configuration compatibility requirements comprise device role configuration compatibility requirements.

57.   The method of claim 56, wherein the device role configuration compatibility requirements comprise device role history configuration compatibility requirements.

58.   The method of claim 1, wherein the step of executing the at least one unsolicited software retrieval command is limited to entities having an approved access level to execute the at least one unsolicited software retrieval command.

59.   The method of claim 58, wherein the access to execute the at least one unsolicited software retrieval command is defined in an access control list (ACL).

60.   The method of claim 58, wherein the access control list ACL is defined by domain name server (DNS) address of the network device.

61.   The method of claim 58, wherein the entity executing the at least one unsolicited software retrieval command comprises an agent.

62.   The method of claim 61 wherein the access to the agent is limited according to domain name server (DNS) address of the network device.

63.   The method of claim 9, wherein the software roles compatibility requirements relate to an IP address of the network device.

64. The method of claim 9, wherein the software roles compatibility requirements relate to IP address compatibility requirements.

65. The method of claim 1, wherein the step of determining is based upon an identification of a virtual local area network (VLAN) with which said network device is associated.

IX.   **EVIDENCE APPENDIX**

None.

X.   RELATED PROCEEDINGS APPENDIX

None.